Verfahren und Vorrichtung zum Schutz von Gegenständen oder Informationen gegen unberechtigten Zugriff

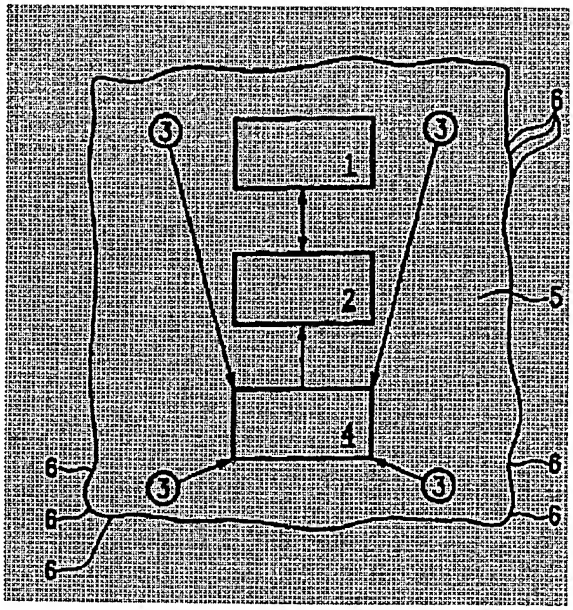
Patent number: DE19855209
Publication date: 2000-06-08
Inventor: WALLERS JOSEPH (DE)
Applicant: DIGITAL DESIGN GMBH (DE)
Classification:
- international: G08B13/22; H05K5/02; G06F12/14
- european: G06F21/00N1T1
Application number: DE19981055209 19981130
Priority number(s): DE19981055209 19981130

Also published as:
WO0033165 (A

Report a data error he

Abstract of **DE19855209**

The invention relates to a method and a device for electronically sealing housings in order to protect objects or information stored inside them against unauthorized or unrecognized access.



Data supplied from the ***esp@cenet*** database - Worldwide

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 55 209 A1**

(51) Int. Cl.[7]:
G 08 B 13/22
H 05 K 5/02
G 06 F 12/14

(21) Aktenzeichen: 198 55 209.2
(22) Anmeldetag: 30. 11. 1998
(43) Offenlegungstag: 8. 6. 2000

(71) Anmelder:
digital design GmbH, 13409 Berlin, DE

(74) Vertreter:
Gulde und Kollegen, 80331 München

(72) Erfinder:
Wallers, Joseph, 10789 Berlin, DE

(56) Entgegenhaltungen:
DE 197 46 421 A1
DE 39 06 122 A1
EP 04 47 615 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Vorrichtung zum Schutz von Gegenständen oder Informationen gegen unberechtigten Zugriff

(57) Gegenstand der Erfindung sind ein Verfahren und eine Vorrichtung zur elektronischen Versiegelung von Gehäusen, um darin verwahrte Gegenstände oder gespeicherte Informationen vor einem unberechtigten oder unerkannten Zugriff zu bewahren. Ein bevorzugtes Anwendungsgebiet der Erfindung ist der Schutz elektronischer Bauteile mit geheimzuhaltenden Schaltungen oder sensiblen Daten oder Programmen.

Der Erfindung lag die Aufgabe zugrunde, ein Verfahren zur Sicherung von Behältnissen verschiedenster Art gegen einen unberechtigten Zugriff bereitzustellen sowie eine Vorrichtung zu dessen Durchführung anzugeben, die innerhalb des zu sichernden Gehäuses angeordnet ist, eine Wiederherstellung durch Fälschung ausschließt und ein Überwachungssignal auslösen kann.

Die Erfindung beruht auf dem Grundgedanken, individuelle, den Schließzustand charakterisierende Merkmale des Gehäuses, das die Gegenstände oder Informationen birgt, zu erfassen und Änderungen dieser Merkmale zu signalisieren.

Dies soll dadurch erreicht werden, daß individuelle Eigenschaften des Gehäuses, eines Teils davon oder mit dem Gehäuse in Wirkverbindung stehender Funktionselemente als Identifikationsmerkmale nach der Inbetriebnahme erfaßt und intern abgespeichert werden, daraufhin kontinuierlich, periodisch oder auf Anforderung die aktuellen Werte gemessen und mit den abgespeicherten Werten verglichen werden, wobei jede signifikante Abweichung

DE 198 55 209 A1

DE 198 55 209 A1

Beschreibung

[Stand der Technik]

Gegenstand der Erfindung sind ein Verfahren und eine Vorrichtung zur elektronischen Versiegelung von Gehäusen, um darin verwahrte Gegenstände oder gespeicherte Informationen vor einem unberechtigten oder unerkannten Zugriff zu bewahren. Die Erfindung ist insbesondere anwendbar zum Nachweis eines unberechtigten Zugriffs auf den Inhalt von Transport- oder Verwahrbehältnissen verschiedenster Art oder zur Kontrolle der Unversehrtheit des Gehäuses von Geräten in der Kommunikations- oder Rechentechnik im Hinblick auf eine mögliche Manipulation. Ein bevorzugtes Anwendungsgebiet der Erfindung ist der Schutz elektronischer Bauteile mit geheimzuhaltenden Schaltungen oder sensiblen Daten oder Programmen vor einem unberechtigten äußeren Zugriff zum Zwecke einer Identifizierung dieser Informationen.

Zur Sicherung von Transport- oder Verwahrbehältnissen mit schützenswertem Inhalt bedient man sich in zahlreichen Technik- und Lebensbereichen sogenannter Siegelsysteme. An dem den Inhalt umschließenden Gehäuse werden Siegelmarken angebracht, ohne deren endgültige Zerstörung das Gehäuse nicht geöffnet werden kann. Verschiedenste Arten und Ausführungsformen solcher Siegelsystem haben eine verbreitete Anwendung gefunden. Der Siegelkörper, der mit für das Öffnen des Gehäuses unumgänglichen Bauteilen in Wirkverbindung steht, umfaßt Gußmassen, Polymer- oder Metallplättchen mit aufgedruckten oder -geprägten Identifikationsmerkmalen.

Diese rein mechanischen Systeme sind wenig zuverlässig, da sie nach einem unbefugten Zugriff durch Fälschung wiederherstellbar sind. Zur Behebung dieses Nachteils existieren Vorschläge, das Siegel mit zusätzlichen Identifikationsmerkmalen auszurüsten. So ist es bekannt, in den Siegelkörper zusätzliche Markierungen in Form von Metallpartikeln in zufälliger Verteilung einzubringen und diese Verteilung mit Hilfe geeigneter Hilfsvorrichtungen zu erfassen und auszuwerten. Des weiteren sind optische Siegel auf der Basis verdrillter Lichtleitfasern beschrieben worden, deren zufälliges Licht raster erfaßt und ausgewertet wird. Ein genereller Nachteil der vorgenannten Systeme ist, daß sie außerhalb des Gehäuses angeordnet sind und damit unmittelbar – mit vorhandenem Fachwissen und geeignetem Werkzeug häufig erfolgreich – attackiert werden können.

Von besonderer Relevanz ist das Problem der Sicherung von Gegenständen oder Informationen gegen unerlaubten Zugriff auf dem Gebiet elektronischer Datenverarbeitungsanlagen. Hier besteht ein Bedürfnis, Bauelemente gegen unautorisierte Eingriffe, deren Ziel es ist, Zugang zu den Schaltungen oder den gespeicherten Daten oder Programmen zu erlangen, zu schützen.

Zur Abwehr solcher Angriffe ist bereits eine Reihe von Maßnahmen bekannt. So ist es übliche Praxis, sensible Informationen zu verschlüsseln und damit nur Personen, die über den entprechenden Schlüssel verfügen, in die Lage zu versetzen, diese Informationen zu lesen und gegebenenfalls zu verändern. Entsprechende Algorithmen sind bekannt und in Benutzung.

Obwohl die gespeicherten Informationen in aller Regel gut geschützt sind, ist es ein genereller Schwachpunkt dieser softwareseitigen Schutzmaßnahmen, daß sie mit entsprechendem Fachwissen durch direkten Zugriff auf die betreffenden Komponenten umgangen werden können. Durch mechanischen oder chemischen Angriff auf das Gehäuse der in Frage kommenden Bauteile, bspw. eines Mikroprozessors, werden diese freigelegt und daraufhin in ihrem Strukturaufbau analysiert.

Eine andere Gattung von Schutzmaßnahmen beruht daher auf solchen Mitteln, die Versuche eines mechanischen oder chemischen Eindringens in sensible Bereiche erkennen und darauf reagieren. Diese Reaktion kann sehr unterschiedlich ausfallen und vom Auslösen eines Alarmsignals bis zum Löschen oder Zerstören der vor unberechtigtem Zugriff zu schützenden Informationen oder Schaltungen reichen.

Zu diesen bekannten hardwareseitigen Lösungen gehört das Umhüllen mit elektrischen Leitern, die auf Unterbrechung, Kurzschluß oder Änderung des Widerstands überwacht werden. Da die Überwachung unabhängig von der äußeren Stromzufuhr möglich sein soll, werden diese Einrichtungen aus zusätzlichen Batterien oder Akkumulatoren versorgt. So schlägt EP 0 417 447 A2 eine Einrichtung zum Schutz elektronischer Schaltungen gegen einen unberechtigten Zugriff mit mechanischen oder chemischen Mitteln vor, wobei die zu schützenden Bauelemente von einem Schutzmantel umgeben sind, auf dem in unmittelbarer Nähe zueinander elektrische Leiter ausgebildet sind. Der Zugang zu den zu schützenden Baugruppen kann nicht ohne Zerstörung zumindest eines oder eines Teils dieser Leiter erreicht werden. Die Wirkung dieser Sicherheitseinrichtung beruht darauf, daß die elektrischen Leiter ständig mit elektrischen Signalen beaufschlagt werden, die ausgangsseitig erfaßt werden.

Jede Änderung der elektrischen Eigenschaften infolge eines äußeren Eingriffs und damit einhergehender Zerstörung eines Teils dieser Leiter erzeugt ein geändertes Signal, das von der Überwachungseinrichtung als solches erkannt wird und eine Löschung der gespeicherten Informationen auslöst. Nach weiteren Aspekten dieser Lösung des Standes der Technik kann die Überwachung durch Aufschaltung weiterer Sensoren auch auf die Intensität einwirkender Strahlung oder die Umgebungstemperatur ausgedehnt werden. Nachteilig ist, daß zwischen dem Erkennen eines Angriffs und den Alarmreaktionen eine zeitliche Verzögerung besteht und vor allem, daß das Löschen von Schlüsseln und Daten Energie erfordert. Bekannte Angriffe zur Umgehung dieser Schutzmaßnahmen zielen daher darauf ab, die für die Erkennung des Alarms oder die Steuerung der Alarmreaktionen erforderlichen Bauteile oder deren Energiezufuhr so schnell zu zerstören, daß keine Reaktionen mehr ausgeführt werden können und anschließend die Schlüssel oder die zu schützenden Daten zu lesen.

Die bekannten Lösungen der Standes der Technik sind mit dem Nachteil behaftet, daß sie einer ständigen Bestromung bedürfen, bei Einsatz sehr empfindlicher Sensoren häufig zu Fehlalarmen neigen und relativ aufwendig und kompliziert aufgebaut und damit entsprechend teuer sind.

[Aufgabe der Erfindung]

Der Erfindung lag die Aufgabe zugrunde, ein Verfahren zur Sicherung von Behältnissen verschiedenster Art gegen einen unberechtigten Zugriff bereitzustellen sowie eine Vorrichtung zu dessen Durchführung anzugeben, die innerhalb des zu sichernden Gehäuses angeordnet ist, eine Wiederherstellung durch Fälschung ausschließt und ein Überwachungssignal auslösen kann.

Insbesondere lag der Erfindung die Aufgabe zugrunde, eine solche Lösung bereitzustellen, die auch auf den Schutz elektronischer Bauteile gegen unzulässige Eingriffe auf geheimzuhaltende Daten, Programme oder Schaltungen übertragbar ist. Erfindungsgemäß wird diese Aufgabe durch ein Verfahren und eine Vorrichtung der in den Ansprüchen 1 und 10 genannten Art gelöst. Vorteilhafte Weiterbildungen der Erfindung geben die Unteransprüche wieder.

Die Erfindung beruht auf dem Grundgedanken, individuelle, den Schließzustand charakterisierende, von außen nicht vermeßbare Merkmale des Gehäuses, das die Gegenstände oder Informationen birgt, zu erfassen und Änderungen dieser Merkmale zu signalisieren. Dies soll dadurch erreicht werden, daß individuelle Eigenschaften des Gehäuses, eines Teils davon oder mit dem Gehäuse in Wirkverbindung stehender Funktionslemente als Identifikationsmerkmale nach der Inbetriebnahme erfaßt und intern abgespeichert werden, daraufhin kontinuierlich, periodisch oder auf Anforderung die aktuellen Werte gemessen und mit den abgespeicherten Werten verglichen werden, wobei jede signifikante Abweichung ein Alarmsignal auslöst. Als Identifikationsmerkmale dienen mit physikalischen, insbesondere optischen, elektrischen, magnetischen oder akustischen Methoden erfaßbare Eigenschaften des Gehäuses, Teilen desselben oder mit dem Gehäuse in Wirkverbindung stehender Funktionselemente innerhalb des lückenlos umschlossenen Raumes. Die Identifikationsmerkmale können aus Zufälligkeiten des Herstellungsprozesses resultieren oder gezielt in Form einer Kodierung aufgebracht worden sein.

Die Vorrichtung zeichnet sich dadurch aus, daß der zu schützende Inhalt zusammen mit einem Überwachungselement in dem Gehäuse untergebracht ist. Das Überwachungselement umfaßt vorzugsweise Sensoren, einen Sicherheitsbaustein und eine Meßschaltung. Dabei dienen die Sensoren der Erfassung der Identifikationsmerkmale des Gehäuses, die, wie nachfolgend noch näher ausgeführt werden wird, bei Inbetriebnahme im Sicherheitsbaustein abgespeichert werden, und im weiteren Verlauf in der Meßschaltung die aktuellen und die gespeicherten Werte verglichen werden. Während das Erfassen der Identifikationsmerkmale stets innerhalb des geschützten Gehäuses erfolgt, können die Vorgänge des Speicherns und Vergleichens auch extern verarbeitet werden. In diesem Falle besitzt das Überwachungselement technische Mittel zum Verschlüsseln und Übertragen der von den Sensoren erfaßten Merkmale. Das Gehäuse ist so konzipiert, daß die von den Sensoren zu erfassenden Merkmale von außen nicht vermeßbar sind und bei jedem Zusammenbau zwangsläufig anders ausfallen. Günstige Gestaltungsmöglichkeiten, die dies gewährleisten, sind in den Ausführungsbeispielen dargelegt.

Nach dem Zusammenbau wird die Vorrichtung aktiviert. Die Sensoren erfassen die individuellen Merkmale des von ihnen beaufschlagten Bereiches und leiten sie an den Sicherheitsbaustein weiter, der die gewonnenen Werte abspeichert. Die Schutzwirkung ist nun aktiv. Kontinuierlich, periodisch, nach jedem Neustart oder auf Anforderung erfaßt die Meßschaltung mit Hilfe der Sensoren die Identifikationsmerkmale des Gehäuses und vergleicht die gemessenen Werte mit denjenigen, welche im Speicher abgelegt sind. Wird das Gehäuse geöffnet oder zerstört, so verändern sich dadurch die Merkmale, die die Sensoren übermitteln. Der Sicherheitsbaustein erkennt diese Veränderung beim Vergleich mit den im Speicher abgelegten Werten und löst ein Alarmsignal aus. Die Art des ausgelösten Signals hängt dabei von den Erfordernissen des Anwendungsfalls ab. In einigen Fällen kann die Markierung eines erfolgten Angriffs über eine Zustandsanzeige genügen, in anderen kann die Benachrichtigung einer Überwachungsstation angezeigt sein. Für Anwendungen zum Schutz von Baugruppen mit geheimzuhaltenden Informationen kann die Auslösung eines Schutzmechanismus bewirkt werden. Entweder das Alarmsignal veranlaßt die Löschung wichtiger Daten oder Programme, oder es markiert den festgestellten Angriff durch das Durchschmelzen einer Sicherung oder durch physikalische Zerstörung oder verweigert dem zu schützenden Bauteil den Zugang zu den in ihm vor der Löschung enthaltenen Funktionen und/oder Daten.

Eine Täuschung des Sicherheitsbausteins nach der Öffnung oder Zerstörung des Gehäuses durch Vorspielung der Merkmale ist nicht möglich, da die Merkmale dazu dem Angreifer bekannt sein müßten. Aber durch ein entsprechendes Konzept einer Gehäusegestaltung wird dafür Sorge getragen, daß die Merkmale bei jedem Zusammenbau unterschiedlich ausfallen oder einer hohen Anzahl möglicher Varianten entstammen, dabei aber von außen weder erkennbar noch meßbar sind und bei jedem Zugriff zwangsläufig verändert werden.

Die Erfindung ist einfach und preisgünstig zu realisieren und universell einsetzbar. Einsatzbereiche sind Behältnisse verschiedenster Art und Dimension, so Transport- oder Verwahrbehältnisse, wie Koffer, Frachtcontainer oder Schließfächer, Sicherheitsräume oder Gehäuse von Rechnern oder Telekommunikationsgeräten oder Umhüllungen elektronischer Bauteile.

Ihre Sicherheit gegen unerkannte Überwindung liegt darin begründet, daß die Identifikationsmerkmale ausschließlich innerhalb der versiegelten Umhüllung gemessen werden, dabei von außerhalb der Umhüllung nicht eingesehen, gemessen oder nach Zugriff geschlußfolgert und wiederhergestellt werden können.

[Beispiele]

Weitere Einzelheiten und Vorteile der Erfindung seien nachfolgend in Ausführungsbeispielen anhand der Zeichnungen dargelegt und näher erläutert.

Hierbei zeigen

Fig. 1 Darstellung des prinzipiellen Aufbaus einer erfindungsgemäßen Vorrichtung, angewandt zum Schutz einer elektronischen Baugruppe;

Fig. 2 Schema des Verfahrensablaufs;

Fig. 3 Schematische Darstellung eines Sicherheitsbausteins;

Fig. 4 Schnittdarstellung einer ersten Ausführungsvariante eines Sicherheitsmoduls für eine zu schützende Baugruppe;

Fig. 5 Schnittdarstellung einer alternativen Ausführungsvariante eines Sicherheitsmoduls;

Fig. 6 Darstellung einer Ausführungsform für ein Verwahrbehältnis;

Fig. 7 Darstellung einer Ausführungsform für ein Transportbehältnis;

Fig. 8 Alternative Ausführungsform zu dem Verfahrensablauf gemäß **Fig.** 2 für eine mehrfache Initialisierung.

Fig. 1 skizziert den prinzipiellen Aufbau eines erfindungsgemäßen Moduls zum Schutz einer elektronischen Baugruppe mit geheimzuhaltenden Schaltungen oder Programmen vor unerlaubtem Zugriff.

Das zu schützende Bauteil (**1**) ist zusammen mit Sensoren (**3**), einem Sicherheitsbaustein (**2**) und einer Meßschaltung (**4**) in einer Umhüllung (**5**) untergebracht. Letztere kann beispielsweise ein aus miteinander in Eingriff stehenden Schalen zusammengesetztes Gehäuse, eine Vergußmasse oder eine Folie sein. Diese Umhüllung (**5**) weist zumindest in einem von den Sensoren (**3**) kontrollierten Bereich markante individuelle Merkmale (**6**) auf, die, wie vorstehend erwähnt, aus einer gezielt aufgebrachten Kodierung oder einer zufällig im Herstellungsprozeß entstandenen Inhomogenität resultieren können. In einer bevorzugten Ausführungsform der Erfindung betreffen diese individuellen Unterscheidungsmerkmale (**6**) der Umhüllung (**5**) optische oder elektrische Parameter. Die Sensoren (**3**) dienen der Erfassung der individuellen Merkmale der Umhüllung (**5**), die im Sicherheitsbaustein bei Inbetriebnahme abgespeichert wer-

den. Die Meßschaltung (4) vergleicht die aktuellen und die abgespeicherten Werte. Der Sicherheitsbaustein (2) ist ein Chip mit einem programmierbaren Festspeicher (13), einem Vergleicher (12) und Funktionen oder Speicher (11), die von dem zu schützenden Bauteil (1) für zentrale Aufgaben, wie Signier- oder Verschlüsselungsdaten oder -algorithmen, benötigt werden (**Fig.** 3). In einer günstigen Ausgestaltungsvariante ist er ein Einchip-Microcontroller mit internem, von außen nicht unmittelbar lesbarem Programm- und Datenspeicher. Der Zugang zu den internen Daten ist nur unter Kontrolle des internen Programms möglich.

Sicherheitsbaustein (2), Sensoren (3) und Meßschaltung (4) können in das zu schützende Bauteil (1) integriert sein.

Beim Zusammensetzen des erfindungsgemäßen Sicherheitsmoduls werden Bauteil (1), Sicherheitsbaustein (2), die Sensoren (3) und Meßschaltung (4) in die Umhüllung (5) eingebracht. Aufgrund der zufälligen oder gezielt eingebrachten Inhomogenitäten des Umhüllungsmaterials oder eines Teils desselben im Wirkbereich der Sensoren (3) fallen bei jedem Zusammenbau die gemessenen Merkmale (6) anders aus. Handelt es sich bei den Inhomogenitäten um gezielt in die Umhüllung (5) eingebrachte Codes, so bestimmen die Sicherheitsanforderungen des konkreten Anwendungsfalls deren erforderliche Anzahl.

Die Wirkungsweise der Vorrichtung ist schematisch in **Fig.** 2 wiedergegeben. Nach dem Zusammenbau befindet sich das Gerät im Initialzustand, das heißt, es sind keine Identifikationsmerkmale im Sicherheitsbaustein (2) gespeichert. Beim ersten Einschalten des Moduls überprüft der Sicherheitsbaustein (2), ob sich der Modul im Initialzustand befindet. Ist dies der Fall, erfassen die Sensoren (3) die optischen, elektrischen oder sonstigen physikalischen Merkmale (6) der Umhüllung (5) und leiten sie an den Sicherheitsbaustein (2) weiter, der die gewonnenen Werte abspeichert. Dabei wird die Kennung für Initialzustand gelöscht. Die Schutzwirkung ist nun aktiv. Bei allen späteren Einschaltvorgängen erfaßt die Meßschaltung (4) mit Hilfe der Sensoren (3) die Merkmale (6) der Umhüllung (5) und vergleicht die gemessenen Werte mit denjenigen, welche im Speicher (13) abgelegt sind. Weichen die Werte signifikant voneinander ab, so löst der Sicherheitsbaustein (2) ein Alarmsignal aus, beispielsweise indem er wichtige Daten oder Programme löscht. In einer bevorzugten Weiterbildung der Erfindung wird die Überwachungsmaßnahme während des Betriebes der zu schützenden Baugruppe (1) periodisch wiederholt. Die Länge der Periode ergibt sich dabei aus den Sicherheitsanforderungen des Anwendungsfalls. Dies gewährleistet, daß auch Angriffe, die während des Betriebes erfolgen, erkannt werden.

Wird die Umhüllung (5) geöffnet oder zerstört, so verändern sich dadurch die Merkmale, die die Sensoren (3) übermitteln. Der Sicherheitsbaustein (2) erkennt diese Veränderung beim Vergleich mit den im Speicher (13) abgelegten Werten. Eine Täuschung des Sicherheitsbausteins (2) nach der Öffnung oder Zerstörung der Umhüllung (5) durch Vorspielung der Merkmale ist nicht möglich, da die Merkmale dazu dem Angreifer bekannt sein müßten. Dies ist jedoch nahezu unmöglich, da nach der Erfindung die Umhüllung (5) so zu konzipieren ist, daß die von den Sensoren (3) erfaßten Identifikationsmerkmale (6) bei jedem Zusammenbau unterschiedlich ausfallen oder einer hohen Anzahl möglicher Varianten entstammen, dabei aber von außen weder erkennbar noch meßbar sind und bei jedem Zugriff oder Versuch eines Zugriffs zwangsläufig verändert werden. Eine favorisierte Ausführungsvariante eines Gehäusekonzepts, basierend auf miteinander verschraubten Gehäuseschalen, gibt **Fig.** 4 wieder. Das Gehäuse umfaßt eine Oberschale (21) und eine Unterschale (22). Mittels mindestens einer Befestigungsschraube (23) sind die Gehäuseschalen (21) und (22) miteinander verbunden. Während die Oberschale (21) einen in den Innenraum ragenden Führungszylinder (7) mit Durchgangsbohrung für den Schraubenschaft (23) aufweist, ist in der Unterschale (22) koaxial ein Führungszylinder (8) mit Innengewinde angeordnet. Der zwischen den Führungszylindern (7) und (8) liegende Bereich des Schraubenschaftes (23) nimmt eine Scheibe (24) auf. Die Scheibe (24) besteht aus einem elastischen Material, vorzugsweise einem Polymeren oder aus Pappe. Durch eine zentrale Bohrung mit einem gegenüber dem Schraubenschaft (23) leicht geringeren Durchmesser wird eine kraftschlüssige Verbindung hergestellt, die die Scheibe (24) der Drehbewegung der Befestigungsschraube (23) folgen läßt. Beim Eindrehen der Schraube (23) in die Unterschale (22) dreht sich die Scheibe (24) so lange mit, bis sie durch die aufeinander zulaufenden Führungszylinder (7) und (8) schließlich eingeklemmt und durch Reibwirkung am Weiterdrehen gehindert wird. Sie hat damit ihre Betriebsstellung erreicht. Die Scheibe (24) ist mit einer Kodierung in Form von Durchbrüchen, Bereichen unterschiedlicher Transparenz oder unterschiedlicher elektrischer Leitfähigkeit ausgerüstet, die die optischen und/oder elektrischen Sensoren (3) im Inneren des Gehäuses (21), (22) zu erfassen vermögen. Die konkrete Stellung der Scheibe (24) ist von außen nicht ersichtlich, da das Gehäuse (21), (22) aus einem undurchsichtigen Material besteht oder entsprechende Beschichtungen aufweist. Auch aus der Stellung der Befestigungsschraube (23) können keine Rückschlüsse auf die konkrete Lage der Scheibe (24) gezogen werden. Da sie beim Eindrehen der Schraube (23) bereits vor dem endgültigen Festziehen am Weiterdrehen gehindert wird, ist ihre Betriebsstellung zufällig. Gleiches gilt für den Fall des Öffnens des Gehäuses (21), (22) durch Aufschrauben. Die Scheibe (24) folgt der Aufschraubbewegung erst, nachdem die Klemmwirkung der Führungszylinder (7) und (8) nachgelassen hat. Aus der Schraubenstellung am geöffneten Modul kann daher nicht auf die Betriebsstellung der Scheibe (24) geschlossen werden. Diese Lösung gewährleistet, daß die konkrete Betriebsstellung der Scheibe (24) und damit letztlich die im Speicher (13) abgelegten und periodisch abgefragten individuellen Gehäusemerkmale (6) selbst dem mit dem Zusammenbau betrauten Personal verborgen bleiben.

Die Wirkungsweise dieser Ausführungsvariante entspricht der Darstellung in **Fig.** 2. Nach dem Zusammenbau befindet sich der Modul im Initialzustand. Es sind keine Merkmale (6) gespeichert. Beim ersten Einschalten erfassen die Sensoren (3) die optischen und/oder elektrischen Merkmale (6) der Scheibe (24) und leiten sie an den Sicherheitsbaustein (2) weiter, der die gewonnenen Werte abspeichert. Bei jedem erneuten Einschaltvorgang oder periodisch erfaßt die Meßschaltung (4) mit Hilfe der Sensoren (3) die Identifikationsmerkmale der Scheibe (24) und vergleicht diese Werte mit denjenigen, welche im Speicher (13) abgelegt sind. Wird das Gehäuse (21), (22) durch Lösen der Befestigungsschraube (23) geöffnet, bewirkt dies eine Drehung der Scheibe (24). Die Sensoren (3) erfassen daraufhin andere Merkmale (6). Der Sicherheitsbaustein (2) erkennt diese Veränderung beim Vergleich mit den im Speicher (13) abgelegten Werten und löst ein Alarmsignal aus.

Die vorgestellte Ausführungsvariante ist einfach und sehr preiswert. Ihre Schutzwirkung ist allerdings auf solche Eingriffe beschränkt, die durch unberechtigtes Aufschrauben erfolgen. Angriffe, die eine Zerstörung des Gehäuses in Kauf nehmen, werden hiervon nicht erfaßt. Um derartige Eingriffe zu erkennen, bedarf es einer aufwendigeren Sensorik, die weitere Teile des Gehäuses (21) und (22) überwacht.

Eine andere zweckmäßige Ausgestaltung der Erfindung,

die Manipulationen an der umgebenden Umhüllung (5) erkennt, ist in **Fig.** 5 dargestellt.

Die Umhüllung (5) ist eine Vergußmasse mit einer zufallsbedingten Markierung, beispielsweise beruhend auf dispergierten Festkörperteilchen. Die zufallsbedingte Verteilung dieser Festkörper im Matrixmaterial dient als Identifikationsmerkmal (6), das mit geeigneten, hier optischen, Methoden vermessen wird. Die zu schützende Baugruppe (1), der Sicherheitsbaustein (2) die Meßschaltung (4), Fotodioden oder -transistoren (3), Leuchtdioden oder Laser oder Lampen (35) sind mit Hilfe der Vergußmasse mit inhomogenen optischen Eigenschaften zu einem Sicherheitsmodul vergossen. Der Modul weist einen undurchsichtigen Überzug (38), beispielsweise einen Farbauftrag, auf. Die zufällig aus den optischen Eigenschaften der Vergußmasse in den Wegen zwischen den lichtaussenden Leuchtdioden (35) und den lichtmessenden Fotodioden (3) resultierenden optischen Verhältnisse, gekennzeichnet durch Dämpfung und Reflexionen, werden gemessen und abgespeichert. Das Ausmessen der optischen Merkmale geschieht dadurch, daß die einzelnen Leuchtdioden (35) nacheinander einzeln oder in Gruppen bestromt werden, und die Fotodioden (3) die Stärke des einfallenden Lichtes an ihren jeweiligen Standorten erfassen. Um Meßfehler durch Temperatur- und Spannungsschwankungen auszugleichen, können diese Messungen auch auf das Bestimmen der relativen Helligkeiten beschränkt werden.

Zur Wirkungsweise der vorstehend beispielhaft dargestellten Ausführungsform sei unter Hinweis auf **Fig.** 2 auf die Darlegungen im Beschreibungsteil und im vorangegangenen Ausführungsbeispiel verwiesen.

Während die Schutzschaltungen in bekannten Geräten des Standes der Technik immer, selbst bei abgeschaltetem Gerät, aktiv sein müssen und daher einer ständigen Bestromung bedürfen, kommt die erfindungsgemäße Lösung ohne ständige Bestromung aus. Dies gestattet einen Verzicht auf zusätzliche Batterien oder Akkumulatoren zur Gewährleistung der Stromversorgung. Deren periodischer Austausch, Wartung und Entsorgung entfallen damit ebenfalls.

Darüber hinaus ist auch die Gefahr von Fehlalarmen gemindert. Grundsätzlich sind die Sensoren so empfindlich ausgelegt, daß jeder Angriff erkannt wird. Dies hät aber gleichzeitig zur Folge, daß Vorgänge in der Umgebung des Gerätes die Sicherheitseinrichtung beeinflussen und als Angriff fehlinterpretiert werden. Da die erfindungsgemäßen Module nur während des Betriebes aktiv sein müssen, entfallen die bei den Lösungen des Standes der Technik häufig zu beobachtenden Fehlalarme außerhalb des Betriebes.

Hervorzuheben ist, daß nach einer Zerstörung des Überwachungselements ein Zugriff auf die zu schützenden Daten, Programme oder Schaltungen ausgeschlossen ist.

Eine weitere günstige Ausführungsform der Erfindung gemäß **Fig.** 6 bezweckt den Schutz des Inhalts eines Verwahrbehältnisses vor unerkanntem Zugriff. Ein Verwahrbehältnis umfaßt zwei in Eingriff stehende Gehäuseschalen (21) und (22). Der von den Schalen (21) und (22) lückenlos umschlossene Raum nimmt Bereich (28) für den zu schützenden Inhalt und das Überwachungselement, bestehend aus mindestens einem Sensor (3), dem Sicherheitsbaustein (2), der Meßschaltung (4) und einer Zustandsanzeige (26), auf. Die Gehäuseschalen (21), (22) werden miteinander in Eingriff gebracht und mittels Schrauben (23) fest zusammengefügt. Mindestens eine der Schrauben (23) nimmt dabei eine beispielsweise mit einem optischen Code ausgerüstete Scheibe (24) auf, welche wiederum im Bereich eines Sensors (3), der den aufgebrachten Code zu lesen vermag, angeordnet ist. Die Wirkungsweise dieser Ausführungsform entspricht im Prinzip der im ersten Ausführungsbeispiel vorgestellten Variante. Bei der Inbetriebnahme erfassen die Sensoren (3) die aufgebrachte Kodierung der Kodierscheibe (24) in dem ihnen zugeordneten Bereich und leiten sie dem nachgeschalteten Sicherheitsbaustein (2) zu, der sie abspeichert. Im weiteren Verlauf werden die ermittelten Informationen durch Vergleich mit den bei der Inbetriebnahme im Sicherheitsbaustein (2) abgespeicherten Werten ausgewertet. Weichen die Merkmale voneinander ab, so wird ein Angriff vermutet und durch geeignete physikalische Maßnahmen, die ein akustisches oder optisches oder an eine Überwachungsstation ausgesandtes Signal sein können, markiert. In der Figur ist zur Anzeige eines ausgelösten Alarmsignals eine in das Gehäuse integrierte Leuchte (26) vorgesehen. Bezugszeichen (27) symbolisiert die Energiezufuhr. Gerade in solchen Anwendungsfällen der elektronischen Versiegelung von Gehäusen, die es angezeigt erscheinen lassen, in einer zentralen Überwachungsstation Informationen über den Zustand dieser Einrichtungen zusammenzufassen, können die Funktionen des Abspeicherns und Vergleichens der Identifikationsmerkmale aus dem Gehäuseinneren in diese Zentrale verlagert werden. Die von den Sensoren im geschützten Gehäuse erfaßten Merkmale werden verschlüsselt, nach außen zur Zentrale übertragen und dort gespeichert und verglichen. Der Begriff "Verschlüsseln" ist dabei weit auszulegen und soll bspw. auch das Hashen umfassen, das – anders als eine Verschlüsselung – keine Rücktransformation (Dekomprimierung und Entschlüsselung) erlaubt.

Verfahren zur sicheren Übermittlung von Daten, in diesem Falle der Sensorwerte, sind Stand der Technik und bedürfen hier an sich keiner weitergehenden Erörterung. Es sei lediglich erwähnt, daß bei der Auswahl des Verfahrens die Möglichkeit eines Replay-Angriffs in Betracht zu ziehen ist. Um zu verhindern, daß ein Angreifer das übertragene Datenpaket abhört, die Übertragung weiterer Messungen unterbricht und der Zentrale während eines Angriffs die abgehörten Werte vorspielt, kommen daher solche Verfahren in Betracht, die vor der Verschlüsselung in das zu übermittelnde Datenpaket sich verändernde Datenfelder (z. B. Datum, Uhrzeit, Zähler oder vorgegebene Werte (Challenge)) einsetzen. In der Zentrale werden das eingehende Paket entschlüsselt, die Sensorwerte verglichen und das zugefügte Datenfeld auf Plausibilität überprüft. Die Übertragung findet über eine Datenleitung, wie z. B. analoge Telefonleitung mit Modem oder über ISDN statt. Die Aufgaben in der Zentrale (Vergleichen, Speichern, Alarm auslösen) werden von einem Computer erledigt.

Der Begriff Verwahrbehältnis ist im vorangegangenen Ausführungsbeispiel im weitesten Sinne auszulegen, insbesondere sind darunter auch Gerätegehäuse zu verstehen. So kann es sich hierbei auch um das Gehäuse eines PC handeln, der vor physikalischer Manipulation zu schützen ist, oder bei dem der Versuch einer solchen Manipulation nachweisbar sein soll. Es kann sich dabei auch um ein Telekommunikationsgerät handeln, das unberechtigtes Öffnen des Gehäuses nachweist, bspw. als Abwehrmaßnahme gegen die Möglichkeit eines Abhörens. Ein sinnvoller Anwendungsfall der letztgenannten Ausführungsvariante des externen Speicherns und Vergleichens ist ein Bankterminal.

Das Verschließen von Transportbehältnissen mittels Schrauben ist in der Handhabung unbequem. Für derartige Behältnisse wird alternativ die in **Fig.** 7 skizzierte Ausführungsform favorisiert. Der Transportbehälter besitzt zwei in Eingriff stehende Gehäuseteile (21) und (22). Er ist in an sich bekannter Weise mit mindestens einem Schließelement ausgestattet. Das innerhalb des Gehäuses (21), (22) untergebrachte Überwachungselement soll wiederum auf einer im Einwirkungsbereich eines Sensors (3) drehbar angeordneten Kodierscheibe (24) als Informationsträger beruhen. Eines

der beiden Gehäuseteile, – in der Figur Schale (**22**) – nimmt Sicherheitsbaustein (**2**) sowie Sensor (**3**) und die drehbare Kodierscheibe (**24**) auf, während das komplementäre Gehäuseteil – in der Figur Schale (**21**) – eine der Kodierscheibe (**24**) eine Drehbewegung auferlegende Zunge (**41**) aufnimmt. Beim Schließen oder Öffnen des Behältnisses tritt die Zunge (**41**) in Reibverbindung mit Welle (**43**). Die Relativbewegung der beiden Gehäuseschalen (**21**) und (**22**) erzeugt eine Drehbewegung der Welle (**43**) und damit auch der Kodierscheibe (**24**). Durch eine keilförmige oder sonstwie mit Unregelmäßigkeiten behaftete Gestaltung der Zunge (**41**) sind Dauer und Intensität des Eingriffs mit Welle (**43**) und damit letztlich die Ruhestellung der Kodierscheibe (**24**) nicht vorhersehbar. Im geschlossenen Zustand drückt die Arretierfläche (**42**) von Zunge (**41**) auf Welle (**43**) und hält sie in ihrer Position.

In Anwendungen, bei denen das Bedürfnis besteht, daß berechtigte Personen oder Maschinen das Gehäuse öffnen, später wieder schließen und die Überwachung neu aktivieren, ist ein Mechanismus integriert, welcher es diesen Personen oder Maschinen erlaubt, die Überwachungsschaltung in den Initialzustand zurückzuversetzen. Der Nachweis der Berechtigung kann durch Eingabe einer PIN, eines Paßworts oder bei höheren Sicherheitsanforderungen auch durch eine kryptographisch abgesicherte Authentifizierung über Schnittstelle (**47**) erfolgen. Die Authentifikation wird vom Sicherheitsbaustein (**2**) durchgeführt, und zwar dergestalt, daß sich der Benutzer gegenüber dem Sicherheitsbaustein (**2**) authentifiziert. Verläuft sie erfolgreich, wird der Sicherheitsbaustein (**2**) in den Initialzustand zurückversetzt. Anderenfalls wird der Alarmzustand ausgelöst (**Fig. 5**).

Patentansprüche

1. Verfahren zur elektronischen Versiegelung von Behältnissen der verschiedensten Art, **dadurch gekennzeichnet**, daß bei Inbetriebnahme individuelle, den Schließzustand charakterisierende, von außen nicht vermeßbare Merkmale des Gehäuses, eines Teils davon oder mit dem Gehäuse in Wirkverbindung stehender Funktionselemente erfaßt und abgespeichert werden, während des Betriebes die Erfassung dieser Identifikationsmerkmale wiederholt wird und die dabei gemessenen Werte mit den abgespeicherten Werten verglichen werden und jede signifikante Abweichung der aktuellen von den abgespeicherten Werten ein Alarmsignal auslöst.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Abspeichern und Vergleichen der Identifikationsmerkmale sowie das Auslösen eines Alarmsignals innerhalb des versiegelten Gehäuses erfolgen.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die innerhalb des versiegelten Gehäuses erfaßten Identifikationsmerkmale verschlüsselt zu einer externen Station übertragen und dort gespeichert und verglichen werden.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Übertragung über eine Datenleitung erfolgt.
5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die wiederholte Erfassung der individuellen Identifikationsmerkmale kontinuierlich, periodisch, bei jedem Neustart oder auf Anforderung erfolgt.
6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß als Identifikationsmerkmale die physikalischen, insbesondere die optischen, magnetischen elektrischen oder akustischen Eigenschaften des Gehäuses, eines Teils davon oder eines mit dem Gehäuse in Wirkverbindung stehenden Funktionselements erfaßt werden.
7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die überwachten Identifikationsmerkmale aus einer zufallsbedingten Markierung oder aus Zufälligkeiten des Herstellungsprozesses resultieren.
8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die überwachten Identifikationsmerkmale eine aufgebrachte Kodierung sind.
9. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Alarmsignal eine Zustandsanzeige ist.
10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Alarmsignal einen Schutzmechanismus für den zu schützenden Inhalt auslöst.
11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß das Alarmsignal eine Löschung gespeicherter Daten oder Programme bewirkt.
12. Verwendung eines Verfahrens nach einem oder mehreren der vorhergehenden Ansprüche zum Schutz elektronischer Bauteile mit geheimzuhaltenden Schaltungen und/oder Daten oder Programmen gegen unautorisierten äußeren Zugriff.
13. Vorrichtung zur elektronischen Versiegelung von Behältnissen der verschiedensten Art, umfassend ein Gehäuse zur lückenlosen Umhüllung eines zu schützenden Inhalts, dadurch gekennzeichnet, daß der zu schützende Inhalt und ein Überwachungselement gemeinsam in dem Gehäuse untergebracht sind und das Überwachungselement über Sensoren (**3**) zur Erfassung individueller, von außen nicht vermeßbarer Merkmale des Gehäuses, eines Teils davon oder mit dem Gehäuse in Wirkverbindung stehender Funktionselemente sowie über mindestens eine Baugruppe (**2, 4**) zum Abspeichern der erfaßten Werte, zum Vergleich der erfaßten und der abgespeicherten Werte und zum Auslösen eines Alarmsignals verfügt.
14. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, daß Baugruppe (**2, 4**) zum Abspeichern und Auswerten der Identifikationsmerkmale sowie zum Auslösen eines Alarmsignals entweder intern, das heißt innerhalb des versiegelten Gehäuses, oder extern, das heißt in einer von dem versiegelten Gehäuse beabstandet angeordneten Station, untergebracht ist.
15. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, daß das Überwachungselement einen Sicherheitsbaustein (**2**), Sensoren (**3**) und eine Meßschaltung (**4**) umfaßt.
16. Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, daß der Sicherheitsbaustein (**2**) ein Chip mit einem programmierbaren Festspeicher (**13**), einem Vergleicher (**12**) und Funktionen oder Speicher für Signier- und Verschlüsselungsdaten oder -algorithmen (**11**) ist.
17. Vorrichtung nach Anspruch 16, dadurch gekennzeichnet, daß der Sicherheitsbaustein (**2**) ein Einchip-Microcontroller mit internem, von außen nicht unmittelbar lesbarem Programm- und Datenspeicher ist.
18. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, daß das Gehäuse miteinander in Eingriff stehende Gehäuseschalen (**21**),(**22**) umfaßt.
19. Vorrichtung nach Anspruch 18, dadurch gekennzeichnet, daß die Gehäuseschalen (**21**), (**22**) miteinander verschraubt sind und mindestens eine der die Gehäuseschalen (**21**) und (**22**) zusammenhaltenden Schrauben (**23**) innerhalb des Gehäuses im Wirkbereich des Sensors (**3**) kraftschlüssig mit einer Kodierscheibe (**24**) verbunden ist.
20. Vorrichtung nach Anspruch 18, dadurch gekenn-

zeichnet, daß Gehäuseschale (**22**) im Wirkbereich des Sensors (**3**) eine drehbeweglich gelagerte Kodierscheibe (**24**) und Gehäuseschale (**21**) eine beim Öffnungs- und Schließvorgang der Kodierscheibe (**24**) eine Drehbewegung auferlegende Zunge (**41**) aufweist, wobei die Zunge (**41**) derart unregelmäßig geformt ist, daß der Eingriff mit der Kodierscheibe (**24**) von wechselnder Intensität ist.

21. Vorrichtung nach Anspruch 20, dadurch gekennzeichnet, daß Zunge (**41**) keilförmig ausgebildet ist.

22. Vorrichtung nach Anspruch 19 oder 20, dadurch gekennzeichnet, daß die optischen oder elektrischen Eigenschaften der Kodierscheibe (**24**) als Identifikationsmerkmale dienen.

23. Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, daß das Gehäuse eine Vergußmasse ist.

24. Vorrichtung nach Anspruch 23, dadurch gekennzeichnet, daß die Vergußmasse eine zufallsbedingte Markierung, beispielsweise in Form dispergierter Festkörper aufweist.

25. Vorrichtung nach Anspruch 24, dadurch gekennzeichnet, daß die optischen Eigenschaften der Vergußmasse als Identifikationsmerkmale dienen.

26. Vorrichtung nach Anspruch 25, dadurch gekennzeichnet, daß eingegossene Leuchtdioden (**35**) und Fotodioden (**3**) die optischen Eigenschaften der Vergußmasse erfassen.

27. Verwendung einer Vorrichtung nach einem oder mehreren der vorhergehenden Ansprüche als Sicherheitsmodul zum Schutz elektronischer Bauteile mit geheimzuhaltenden Schaltungen und/oder Daten oder Programmen gegen unautorisierten äußeren Zugriff.

Hierzu 6 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

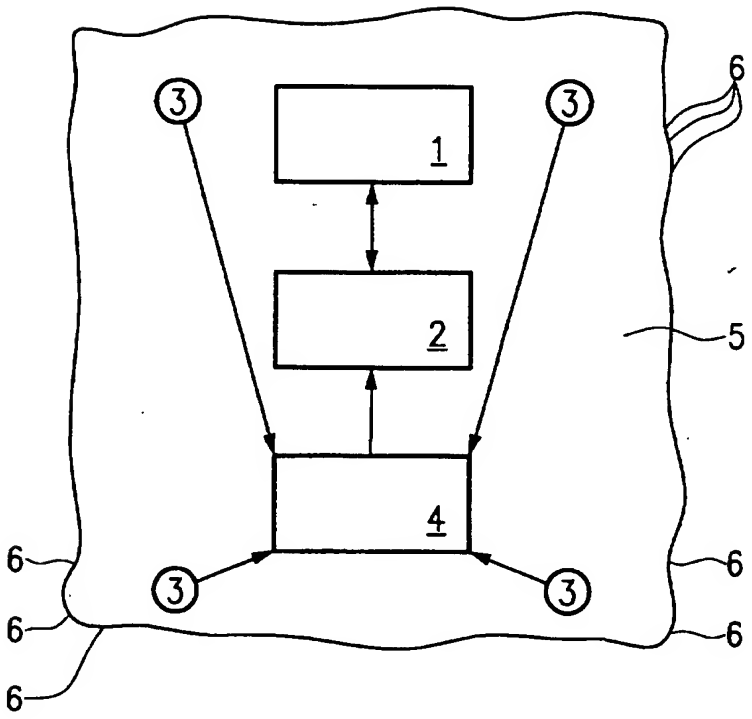


FIG. 1

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

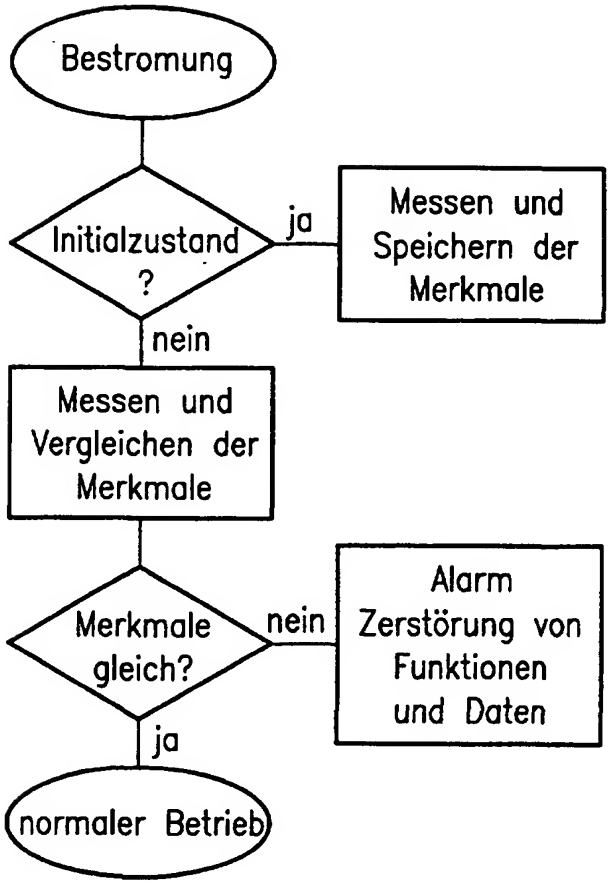


FIG.2

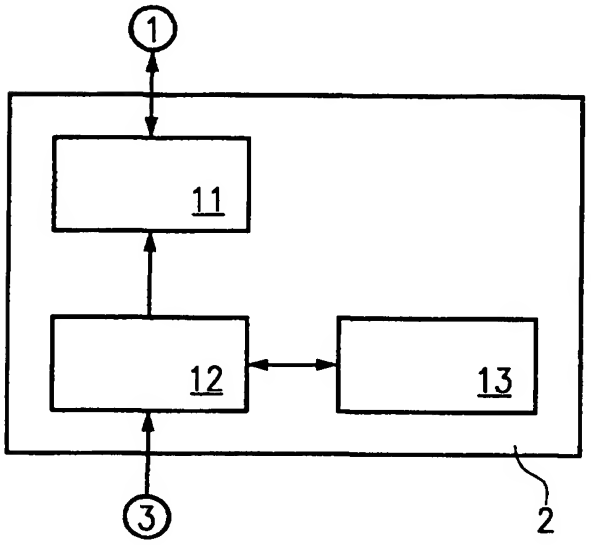


FIG.3

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

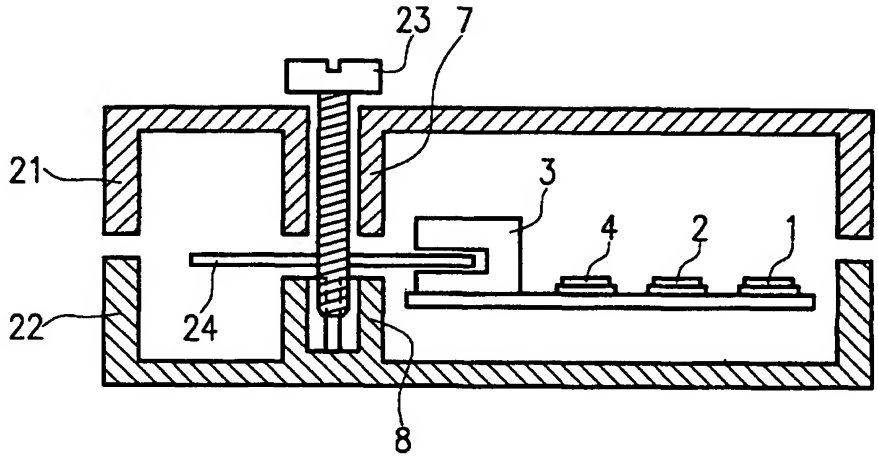


FIG.4

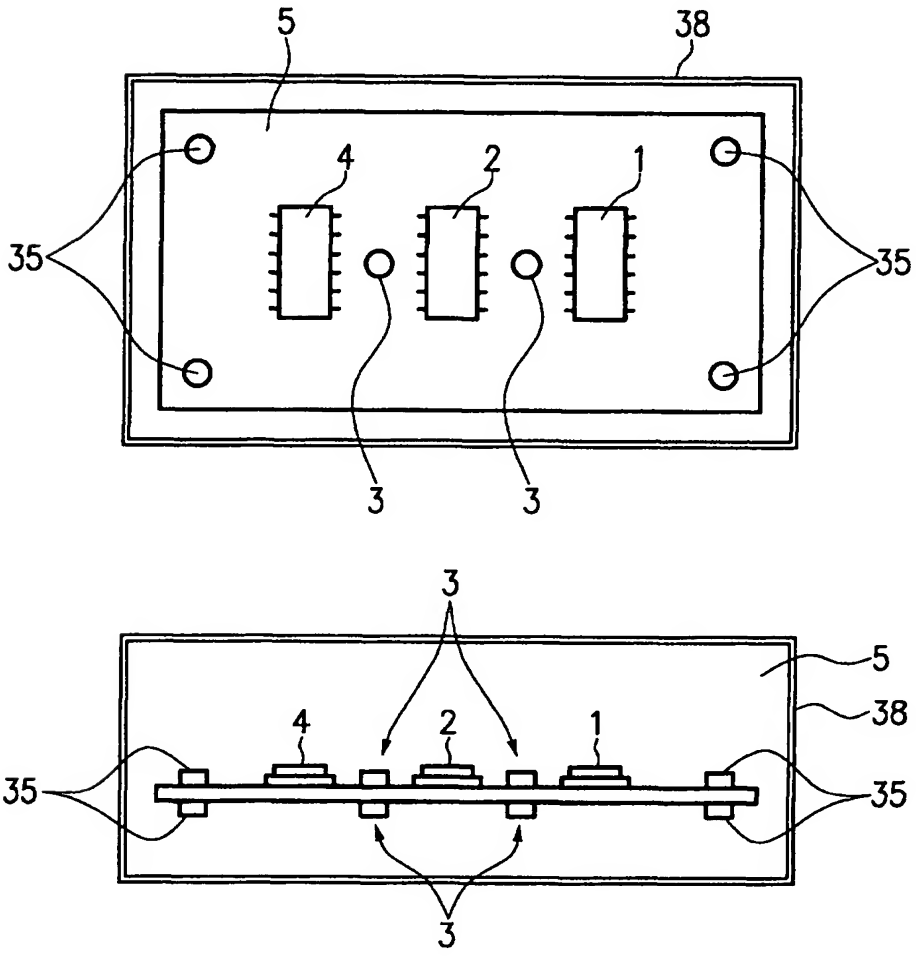


FIG.5

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

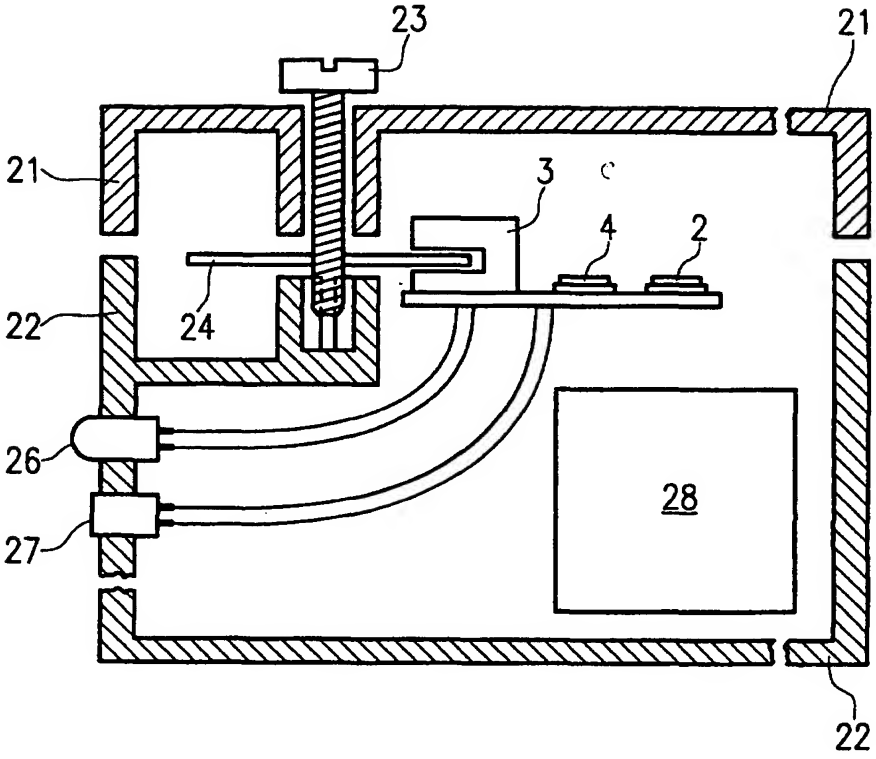


FIG.6

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

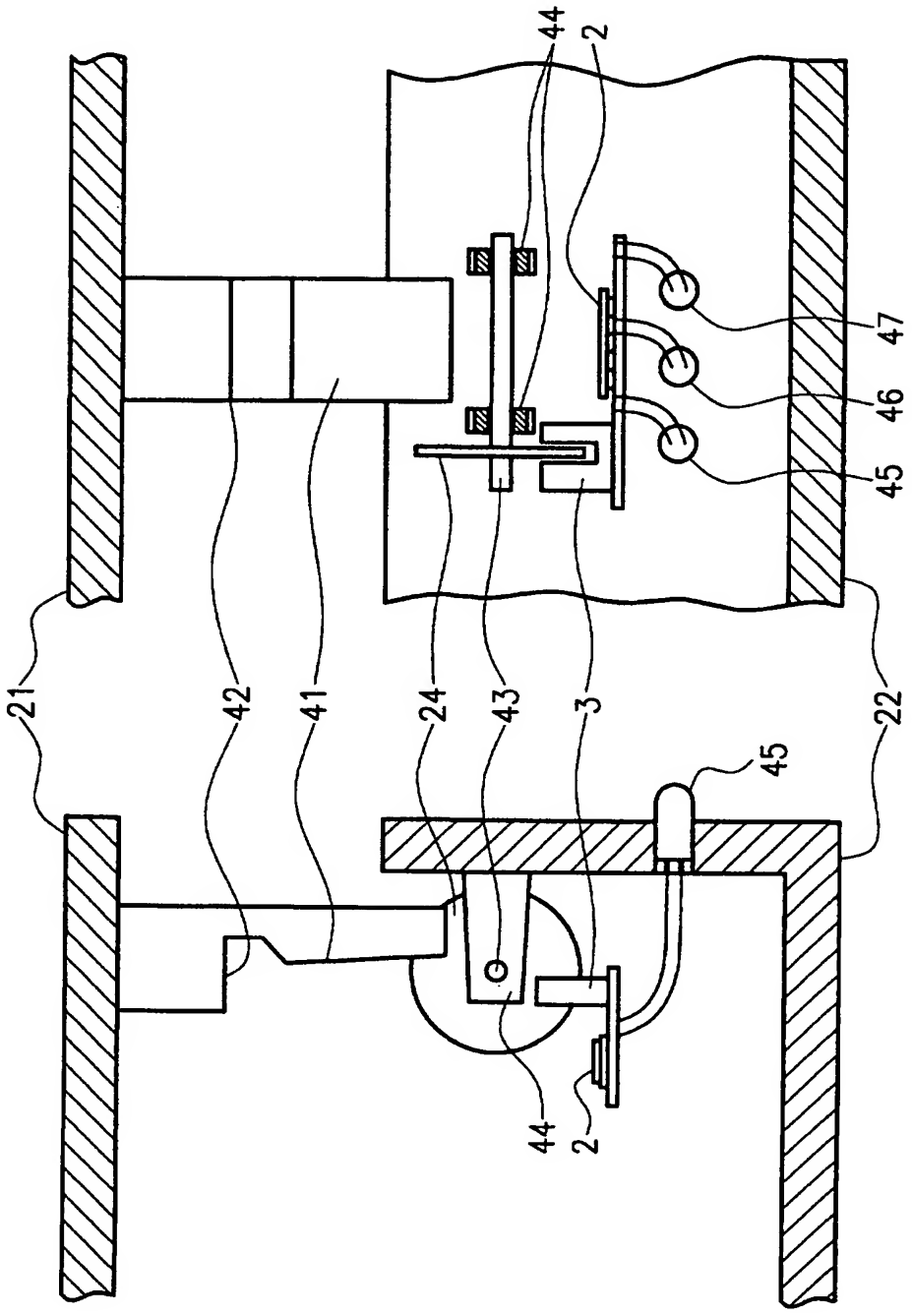


FIG. 7

Nummer: DE 198 55 209 A1
Int. Cl.[7]: G 08 B 13/22
Offenlegungstag: 8. Juni 2000

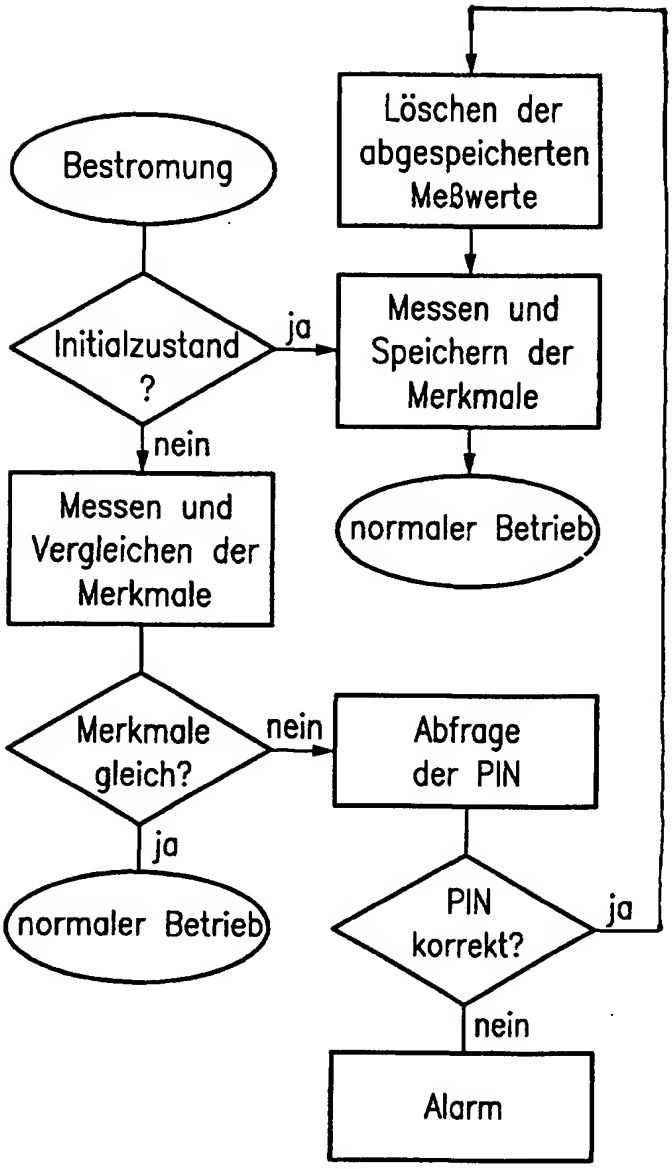


FIG.8